Guida di Desktop Management
Business Desktops

Numero di parte del documento: 312947-062

Settembre 2003

La presente guida fornisce definizioni ed istruzioni delle funzioni di sicurezza d'uso e Intelligent Manageability preinstallate su alcuni modelli.

AVVERTENZA: Il testo presentato in questo modo indica che la mancata osservanza delle istruzioni potrebbe comportare lesioni fisiche o addirittura la perdita della vita.

ATTENZIONE: Il testo presentato in questo modo indica che la mancata esecuzione delle indicazioni fornite potrebbe provocare danni all'apparecchiatura o la perdita di informazioni.

Guida di Desktop Management
Business Desktops

Seconda edizione (Settembre 2003)
Numero di parte del documento: 312947-062

Sommario

Guida di Desktop Management

Configurazione iniziale e deployment 2
Installazione remota del sistema 2
Gestione e aggiornamento del software 3
HP Client Manager Software 3
Soluzioni Altiris 4
Altiris PC Transplant Pro 5
System Software Manager 5
Proactive Change Notification 5
ActiveUpdate 6
Flash su ROM 6
Flash remoto della ROM 7
HPQFlash 7
ROM con blocco di avvio FailSafe 8
Replica delle impostazioni 9
Pulsante d'accensione a due stati 18
Sito World Wide Web 19
Moduli e collaboratori 19
Controllo e sicurezza delle risorse 20
Sicurezza tramite password 24
Impostazione di una password di impostazione tramite Computer Setup 24
Immissione della password di accensione con Computer Setup 25
Sicurezza integrata 29
DriveLock 38
Sensore Smart Cover 41
Chiusura Smart Cover 42
Master Boot Record Security (Sicurezza MBR (Master Boot Record)) 45

Partizionamento e formattazione del disco avviabile corrente 47
Predisposizione per chiusura con cavo 47
Tecnologia per l'identificazione delle impronte digitali. 48
Notifica guasti e ripristino 48
Drive Protection System (DPS) 48
Alimentatore protetto contro gli sbalzi di tensione. 49
Sensore termico. 49

Indice Analitico

Guida di Desktop Management

HP Intelligent Manageability fornisce soluzioni per la gestione e il controllo di PC desktop, workstation e portatili in ambienti di rete basate sui più affermati standard del settore. HP propone soluzioni per la gestione dei desktop fin dal 1995, con l'introduzione sul mercato dei primi personal computer completamente gestibili. HP dispone di una tecnologia di gestione brevettata, grazie alla quale ha condotto un incessante sforzo per sviluppare gli standard e le infrastrutture occorrenti per il deployment, la configurazione e la gestione efficaci di PC desktop, workstation e portatili. Intelligent Manageability è un elemento importante del grande impegno che la Compaq ha posto nella realizzazione di soluzioni per ottimizzare il ciclo vitale del PC, in grado di seguire l'utente nelle quattro fasi della pianificazione, deployment, gestione e transizioni.

Le funzionalità e caratteristiche principali della gestione desktop sono:

- Configurazione iniziale e deployment
- Installazione remota del sistema
- Aggiornamento e gestione del software
- Flash della ROM
- Controllo e sicurezza delle risorse
- Notifica guasti e ripristino

Il supporto di funzioni specifiche descritte in questa guida può variare in base al modello e alla versione del software.

Configurazione iniziale e deployment

Il computer viene fornito con un'immagine del software di sistema preinstallata. Dopo una veloce fase di "scompattamento" del software il computer è pronto per l'uso.

Potrebbe rivelarsi necessario sostituire l'immagine del software preinstallata con un set personalizzato di software applicativi e di sistema. In tal caso, esistono vari metodi per personalizzare il software. È possibile operare come segue:

- Installare il software applicativo aggiuntivo dopo aver scompattato l'immagine del software preinstallata.
- Utilizzare strumenti di deployment come Altiris Deployment Solution™ per sostituire il software preinstallato con un'immagine del software personalizzata.
- Eseguire una procedura di clonazione del disco per copiare il contenuto da un disco fisso ad un altro.

Il metodo di messa in uso da scegliere dipende dai processi e dagli ambienti informatici degli utenti. La sezione PC Deployment (Installazione del PC) del sito Web HP Lifecycle Solutions (Soluzioni relative al ciclo vitale HP) (http://h18000.www1.hp.com/solutions/pcsolutions) fornisce informazioni utili per la scelta del metodo migliore di installazione.

Il CD *Restore Plus!* l'installazione da ROM e l'hardware compatibile ACPI forniscono ulteriore assistenza per il ripristino del software di sistema, la gestione e la soluzione dei problemi di configurazione e la gestione dell'alimentazione.

Installazione remota del sistema

L'installazione remota del sistema consente di avviare e impostare il sistema utilizzando il software e le informazioni di configurazione situati in un server di rete tramite il Preboot Execution Environment (PXE). La funzione di installazione remota del sistema viene di solito utilizzata come strumento di impostazione e configurazione del sistema e può servire ai seguenti scopi:

- Formattazione di un'unità disco rigido
- Installazione di una copia del software su uno o più nuovi PC

- Aggiornamento a distanza del BIOS di sistema nella flash ROM ("Flash remoto della ROM" a pagina 7)
- Configurazione delle impostazioni del BIOS di sistema

Per avviare l'installazione remota del sistema premere **F12** quando viene visualizzato il messaggio F12 = Avvio servizio di rete nell'angolo inferiore sinistro della schermata del logo HP. Per proseguire seguire le istruzioni sullo schermo. La sequenza di avvio predefinita viene configurata nel BIOS e può essere modificata in modo da provare ad avviare sempre da PXE.

HP e Altiris, Inc. si sono associati per poter fornire strumenti progettati per facilitare il compito di unire installazione e gestione del PC con meno dispendio di tempo, riducendo infine i costi totali di proprietà e rendendo i sistemi HP i più gestibili PC client dell'ambiente aziendale.

Gestione e aggiornamento del software

HP ha dotato desktop e workstation di diversi strumenti per la gestione e l'aggiornamento del software, Altiris; Altiris PC Transplant Pro; HP Client Manager Software, una soluzione Altiris; System Software Manager; Proactive Change Notification e ActiveUpdate.

HP Client Manager Software

Intelligent HP Client Manager Software (HP CMS) integra appieno la tecnologia HP Intelligent Manageability in Altiris per fornire funzioni di gestione hardware superiori per dispositivi d'accesso HP, fra cui:

- Elenchi dettagliati dei componenti hardware per la gestione delle risorse
- Monitoraggio e diagnostica dello stato del PC
- Notifica proattiva di modifiche nell'ambiente hardware
- Report accessibile da Web di particolari di estrema importanza, come macchine con sistemi di allarmi di temperatura, di memoria ed altro ancora
- Aggiornamento a distanza di software di sistema, ad esempio driver e BIOS della ROM
- Modifica a distanza della sequenza di avvio

Per ulteriori informazioni su HP Client Manager consultare http://h18000.www1.hp.com/im/client_mgr.html.

Soluzioni Altiris

HP Client Management Solutions prevede la gestione hardware centralizzata dei dispositivi client HP per tutto il ciclo vitale delle apparecchiature informatiche.

- Gestione componenti hardware e risorse
  - Verifica licenze
  - Monitoraggio e reporting PC
  - Monitoraggio cespiti/contratti di leasing
- Installazione e migrazione
  - Migrazione Microsoft Windows 2000 o Windows XP Professional o Home Edition
  - Installazione del sistema
  - Migrazioni personalizzate
- Help Desk e risoluzione dei problemi
  - Gestione richieste di intervento help desk prepagate
  - Individuazione dei problemi a distanza
  - Risoluzione dei problemi a distanza
  - Disaster recovery dei client
- Gestione software e operativa
  - Gestione corrente desktop
  - Installazione software di sistema HP
  - Application self-healing

Su determinati modelli di computer desktop e notebook è previsto un agente di gestione Altiris che fa parte dell'immagine caricata di fabbrica. L'agente consente la comunicazione con Altiris Development Solution, utilizzabile per completare l'installazione di nuovo hardware o migrazione personalizzata ad un nuovo sistema operativo tramite una semplice procedura guidata. Le soluzioni Altiris prevedono funzioni di distribuzione software di facile uso. In abbinamento a SSM, o HP Client Manager, gli amministratori sono anche in grado di aggiornare il BIOS su ROM e i driver di periferica da una consolle centrale.

Per ulteriori informazioni consultare http://www.hp.com/go/easydeploy.

Altiris PC Transplant Pro

Altiris PC Transplant Pro garantisce una migrazione indolore del PC mantenendo le vecchie impostazioni e preferenze e i vecchi dati e trasportandoli in modo semplice e rapido nel nuovo ambiente. L'upgrade richiede solo alcuni minuti, anziché ore o giorni, e il desktop ha l'aspetto e le funzioni previste.

Per ulteriori informazioni e particolari sulle modalità di download di una copia di valutazione valida 30 giorni completa di tutte le funzioni consultare http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

System Software Manager (SSM) è un'utility che consente di aggiornare il software a livello di sistema su più PC contemporaneamente. Se eseguita su un sistema client del PC, SSM rileva le versioni hardware e software, quindi aggiorna il software appropriato attingendo da un apposito archivio centrale. Le versioni dei driver supportati da SSM sono indicate con un'icona particolare nel sito Web dal quale scaricare i driver e sul CD del software di supporto. Per scaricare l'utility o per ulteriori informazioni su SSM consultare http://h18000.www1.hp.com/im/ssmwp.html.

Proactive Change Notification

Il programma Proactive Change Notification utilizza il sito Web Subscriber's Choice per effettuare in modo proattivo ed automatico le seguenti operazioni:

- Invio di messaggi di posta elettronica PCN (Proactive Change Notification) contenenti informazioni sulle modifiche hardware e software alla maggior parte dei computer e server commerciali, con un preavviso massimo di 60 giorni.
- Invio di messaggi di posta elettronica Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins e Driver che segnalano problemi per la maggior parte dei computer e server commerciali.

Creazione di profili personalizzati per ricevere esclusivamente le informazioni relative ad uno specifico ambiente informatico. Per saperne di più sul programma Proactive Change Notification e creare un profilo personalizzato consultare http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate è un'applicazione HP di tipo client, che funziona sul sistema locale e utilizza profili definiti dall'utente per scaricare in modo proattivo ed automatico aggiornamenti software per la maggior parte dei computer e server HP disponibili in commercio. Gli aggiornamenti software scaricati possono essere intelligentemente installati sulle macchine per le quali sono stati previsti da HP Client Manager Software e dal System Software Manager.

Per saperne di più su ActiveUpdate, scaricare l'applicazione e creare un profilo consultare: http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

Flash su ROM

Il computer è dotato di una flash ROM programmabile. Con la definizione di una password di configurazione in Computer Setup (F10) è possibile proteggere la ROM in modo che non venga involontariamente aggiornata o sovrascritta. Si tratta di un aspetto importante per garantire l'integrità operativa del PC. Dovendo o volendo aggiornare la ROM, è possibile:

- Richiedere ad HP un dischetto con ROMPaq aggiornato.
- Scaricare le ultime immagini ROMPaq da http://h18000.www1.hp.com/im/ssmwp.html.

ATTENZIONE: Per garantire la massima protezione della ROM, è bene definire una password di impostazione. La password di impostazione impedisce gli aggiornamenti non autorizzati della ROM. System Software Manager consente all'amministratore di sistema di definire la password di impostazione su uno o più PC contemporaneamente. Per ulteriori informazioni consultare http://h18000.www1.hp.com/im/ssmwp.html.

Flash remoto della ROM

Il flash remoto della ROM consente all'amministratore di sistema di aggiornare in condizioni di sicurezza la ROM dei PC HP remoti direttamente dalla consolle di gestione centralizzata della rete. La possibilità per l'amministratore di sistema di eseguire questa operazione a distanza su più PC si traduce in un deployment coerente e in un maggior controllo delle immagini ROM dei PC HP in rete. Inoltre, ne derivano una maggiore produttività e una diminuzione del costo totale della proprietà.

Per l'esecuzione del flash remoto della ROM, il computer deve essere acceso o attivato tramite l'Apri sessione remoto.

Per ulteriori informazioni sul flash remoto della ROM vedere HP Client Manager Software o System Software Manager su http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

L'utility HPQFlash viene utilizzata per aggiornare localmente o ripristinare la ROM di sistema sui singoli PC tramite un sistema operativo Windows.

Per ulteriori informazioni su HPQFlash visitare http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

ROM con blocco di avvio FailSafe

La ROM con blocco di avvio FailSafe consente il ripristino del sistema nel caso, improbabile, che il flash della ROM non dovesse riuscire, ad esempio in seguito ad interruzione dell'alimentazione durante l'aggiornamento della ROM. Il blocco dell'avvio è una sezione della ROM con protezione flash che effettua un controllo di convalida della ROM ogni volta che il sistema viene acceso.

- Se la ROM di sistema è valida, il sistema parte normalmente.
- Se la ROM di sistema non supera il controllo di convalida, la ROM con blocco di avvio FailSafe fornisce supporto sufficiente per l'avvio del sistema da un dischetto ROMPaq che programmi la ROM con un'immagine valida.

Quando il blocco di avvio rileva una ROM di sistema non valida, il LED di alimentazione di sistema lampeggia di colore ROSSO 8 volte, una al secondo, e fa una pausa di 2 secondi. Contemporaneamente vengono emessi 8 segnali acustici. A video appare un messaggio che indica la modalità di ripristino del blocco di avvio (in alcuni modelli).

Per ripristinare il sistema in modalità di ripristino Boot Block (blocco di avvio) procedere come di seguito indicato:

1. Se nell'unità a dischetti è inserito un dischetto, toglierlo e spegnere il computer.
2. Inserire un dischetto ROMPaq nel lettore.
3. Accendere il sistema.
4. Se non viene rilevato alcun dischetto ROMPaq, il sistema ne richiede l'introduzione ed il riavvio del computer.
5. Se è stata impostata una password di configurazione, la spia del blocco delle maiuscole si accende ed il sistema richiede l'inserimento della password.
6. Digitare la password di configurazione.
7. Se il sistema riesce ad avviarsi dal dischetto e a riprogrammare la ROM, le tre spie della tastiera si accendono. Il successo dell'operazione viene segnalato inoltre da una serie di segnali acustici di tono crescente.

8. Togliere il dischetto e spegnere il computer.
9. Accendere o riavviare il computer.

La seguente tabella elenca le diverse combinazioni delle spie della tastiera utilizzate dalla ROM con blocco di avvio (quando al computer è collegata una tastiera PS/2) con i relativi significati e procedure.

Combinazioni delle spie della tastiera utilizzate dalla ROM con blocco di avvio

Modalità blocco di avvio FailSafe	Colore del LED della tastiera	Tastiera del LED della tastiera	Stato/Messaggio
Bloc Num	Verde	Acceso	Dischetto ROMPaq non presente, danneggiato o non pronto.
Bloc Maiusc	Verde	Acceso	Immettere la password.
Bloc Num, Maiusc, Scorr	Verde	Lampeggiamento sequenziale, uno alla volta: N, C, SL	Tastiera bloccata in modalità rete.
Bloc Num, Maiusc, Scorr	Verde	Acceso	Flash della ROM con blocco dell'avvio eseguito con successo. Spegnere e riaccendere.

✎ Le spie diagnostiche non lampeggiano su tastiere USB.

Replica delle impostazioni

Le seguenti procedure offrono all'amministratore di sistema la possibilità di copiare facilmente le impostazioni di un computer su altri computer dello stesso modello. Ciò consente una configurazione più veloce e uniforme di più computer.

✎ In entrambe le procedure è necessaria un'unità a dischetti oppure un dispositivo flash media USB compatibile, come HP Drive Key.

Copia su computer singolo

ATTENZIONE: La configurazione è specifica per ogni modello. Se i computer d'origine e di destinazione non sono dello stesso modello si può avere corruzione del file system. Non copiare, ad esempio, la configurazione da un D510 Ultra-slim Desktop ad un D510 e-pc.

1. Selezionare una configurazione da copiare. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Inserire un dischetto o un dispositivo flash media USB.
4. Dal menu **File** scegliere **Salva su dischetto**. Per creare il dischetto di configurazione o il dispositivo flash media USB, seguire le istruzioni a video.
5. Spegnere il computer da configurare ed inserire il dischetto di configurazione o il dispositivo flash media USB.
6. Accendere il computer. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.
7. Dal menu **File >** scegliere **Ripristina da dischetto** e seguire le istruzioni a video.
8. Al termine della configurazione, riavviare il computer.

Copia su più computer

ATTENZIONE: La configurazione è specifica per ogni modello. Se i computer d'origine e di destinazione non sono dello stesso modello si può avere corruzione del file system. Non copiare, ad esempio, la configurazione da un D510 Ultra-slim Desktop ad un D510 e-pc.

Questo metodo richiede un po'più di tempo per preparare il dischetto di configurazione o il dispositivo flash media USB, ma la copia della configurazione sui computer di destinazione avviene molto più rapidamente.

In Windows 2000 non è possibile creare un dischetto avviabile, necessario per questa procedura o per creare un dispositivo flash media USB. Se non è possibile utilizzare Windows 9x o Windows XP per creare un dischetto avviabile, utilizzare il metodo di copiatura su un singolo computer (vedere "Copia su computer singolo" a pagina 10).

1. Creare un dischetto avviabile o un dispositivo flash media USB. Vedere "Dischetto avviabile" a pagina 12, "Dispositivi flash media USB supportati" a pagina 13 o "Dispositivi flash media USB non supportati" a pagina 16.

ATTENZIONE: Non tutti i computer possono essere avviati da un dispositivo flash media USB. Se nella sequenza d'avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, significa che è possibile avviare il computer dal dispositivo flash media USB. Altrimenti, si deve utilizzare un dischetto avviabile.

2. Selezionare una configurazione da copiare. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
3. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

4. Inserire un dischetto avviabile o un dispositivo flash media USB.
5. Dal menu **File scegliere Salva su dischetto**. Per creare il dischetto di configurazione o il dispositivo flash media USB seguire le istruzioni a video.
6. Scaricare un'utility BIOS per la replica della configurazione (repset.exe) e copiarla nel dischetto di configurazione o nel dispositivo flash media USB. L'utility si trova su http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. Nel dischetto di configurazione o nel dispositivo flash media USB creare un file autoexec.bat contenente il comando seguente:

   repset.exe

8. Spegnere il computer da configurare. Inserire il dischetto di configurazione o il dispositivo flash media USB e riaccendere il computer. L'utility di configurazione si avvia automaticamente.
9. Al termine della configurazione riavviare il computer.

Creazione di un dispositivo avviabile

Dischetto avviabile

Le istruzioni si riferiscono a Windows XP Professional e Home Edition. Windows 2000 non supporta la creazione di dischetti avviabili.

1. Inserire un dischetto nell'unità a dischetti.
2. Fare clic su **Start/Avvio**, **Risorse del computer**.
3. Fare clic col pulsante destro del mouse sull'unità a dischetti e selezionare **Formatta**.
4. Selezionare la casella di controllo **Crea disco di avvio MS-DOS** e fare clic su **Avvia**.

Ritornare a "Copia su più computer" a pagina 11.

Dispositivi flash media USB supportati

Nei dispositivi supportati, ad esempio HP Drive Key o DiskOnKey, è preinstallata un'immagine che semplifica la procedura necessaria per renderli avviabili. Se il Drive Key in uso non ha tale immagine, utilizzare la procedura riportata più avanti in questa sezione (vedere "Dispositivi flash media USB non supportati" a pagina 16).

ATTENZIONE: Non tutti i computer possono essere avviati da un dispositivo flash media USB. Se nella sequenza d'avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, significa che è possibile avviare il computer dal dispositivo flash media USB. Altrimenti, si deve utilizzare un dischetto avviabile.

Per creare un dispositivo flash media USB avviabile è necessario avere:

- Uno dei seguenti sistemi:
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 Minitower convertibile/Small Form Factor
  - HP Compaq Business Desktop d530 Series – Ultra-slim Desktop, Small Form Factor o Minitower convertibile
  - Notebook Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c o N1000c
  - Notebook Compaq Presario 1500 o 2800

  A seconda del tipo di BIOS, è possibile che in futuro altri sistemi supportino l'avvio da HP Drive Key.

ATTENZIONE: Se non si utilizza un computer presente nell'elenco sopra riportato, verificare che nella sequenza di avvio predefinita dell'utility Computer Setup (F10) il dispositivo USB si trovi prima dell'unità disco rigido.

- Uno dei seguenti moduli di memorizzazione:
  - HP Drive Key da 16 MB
  - HP Drive Key da 32 MB
  - DiskOnKey da 32 MB
  - HP Drive Key da 64 MB
  - DiskOnKey da 64 MB
  - HP Drive Key da 128 MB
  - DiskOnKey da 128 MB

- Un dischetto DOS avviabile con i programmi FDISK e SYS. Se SYS non è disponibile, si può utilizzare FORMAT, ma in questo caso si perderebbero tutti i file esistenti sul Drive Key.

1. Spegnere il computer.
2. Inserire il Drive Key in una delle porte USB del computer e togliere tutti gli altri dispositivi di memorizzazione USB tranne l'unità a dischetti USB.
3. Inserire nell'unità a dischetti un dischetto DOS avviabile con FDISK.COM e SYS.COM o FORMAT.COM e accendere il computer per avviare il dischetto DOS.
4. Per eseguire FDISK da A:\ prompt digitare **FDISK** e premere Invio. Alla richiesta del sistema, fare clic su **Yes** (**Y**) per abilitare la compatibilità con dischi di grandi dimensioni.
5. Inserire l'opzione [**5**] per visualizzare le unità presenti nel sistema. Viene configurata come Drive Key l'unità con dimensioni più simili a quelle di una delle unità elencate. Di solito è l'ultima dell'elenco. Annotare la lettera dell'unità.

   Unità Drive Key: _____

ATTENZIONE: Se nessuna unità non corrisponde al Drive Key, non procedere, potrebbe verificarsi perdita di dati. Verificare tutte le porte USB per ulteriori dispositivi di memorizzazione. Se se ne trovano, toglierli, riavviare il computer e proseguire con il punto 4. Se non se ne trovano, significa che il sistema non supporta il Drive Key o che il Drive Key è difettoso. NON procedere tentando di rendere avviabile il Drive Key.

6. Per uscire da FDISK, premere il tasto **Esc** per ritornare al prompt A:\.
7. Se il dischetto DOS avviabile contiene SYS.COM, passare al punto 8. Altrimenti, passare al punto 9.
8. Al prompt A:\ digitare **SYS x:** dove x rappresenta la lettera dell'unità sopra annotata. Passare al punto 13.

ATTENZIONE: Verificare di avere inserito correttamente la lettera corrispondente al Drive Key.

Una volta trasferiti i file di sistema, SYS ritorna al prompt A:\.

9. Copiare eventuali file da conservare dal Drive Key su una directory temporanea su un'altra unità (ad esempio, l'unità disco rigido interna del sistema).
10. Al prompt A:\ digitare **FORMAT /S X:** dove X rappresenta la lettera dell'unità sopra annotata.

ATTENZIONE: Verificare di avere inserito correttamente la lettera corrispondente al Drive Key.

FORMAT visualizza uno o più messaggi di avvertenza e ogni volta chiede se si vuole procedere. Inserire sempre **y**. FORMAT formatta il Drive Key, aggiunge i file di sistema e richiede l'immissione di un'etichetta di volume.

11. Premere **Invio** per non inserire nessuna etichetta o digitarne l'eventuale testo.
12. Ritrasferire sul Drive Key gli eventuali file salvati al punto 9.
13. Togliere il dischetto e riavviare il computer, che a questo punto considera il Drive Key come unità C.

La sequenza d'avvio predefinita varia da computer a computer, e può essere modificata nell'utility Computer Setup (F10).

Se si è utilizzata una versione DOS di Windows 9x, è possibile che appaia una schermata con il logo di Windows. Per non visualizzarla, aggiungere il file LOGO.SYS vuoto alla directory principale del Drive Key.

Ritornare a "Copia su più computer" a pagina 11.

Dispositivi flash media USB non supportati

ATTENZIONE: Non tutti i computer possono essere avviati da un dispositivo flash media USB. Se nella sequenza d'avvio predefinita nell'utility Computer Setup (F10) il dispositivo USB si trova prima dell'unità disco rigido, significa che è possibile avviare il computer dal dispositivo flash media USB. Altrimenti, si deve utilizzare un dischetto avviabile.

Per creare un dispositivo flash media USB avviabile è necessario avere:

- Uno dei seguenti sistemi:
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 Minitower convertibile/Small Form Factor
  - HP Compaq Business Desktop d530 Series – Ultra-slim Desktop, Small Form Factor o Minitower convertibile
  - Notebook Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c o N1000c
  - Notebook Compaq Presario 1500 o 2800

  A seconda del tipo di BIOS, è possibile che in futuro altri sistemi supportino l'avvio da un dispositivo flash media USB.

ATTENZIONE: Se non si utilizza un computer presente nell'elenco sopra riportato, verificare che nella sequenza di avvio predefinita dell'utility Computer Setup (F10) il dispositivo USB si trovi prima dell'unità disco rigido.

- Un dischetto DOS avviabile con i programmi FDISK e SYS. Se SYS non è disponibile, si può utilizzare FORMAT, ma in questo caso si perderebbero tutti i file esistenti sul Drive Key.

1. Se sul sistema sono installate schede PCI relative ad unità SCSI, ATA RAID o SATA, spegnere il computer e scollegare il cavo d'alimentazione.

ATTENZIONE: Il cavo d'alimentazione DEVE essere scollegato.

2. Aprire il computer e togliere le schede PCI.
3. Inserire il dispositivo flash media USB in una delle porte USB del computer e togliere tutti gli altri dispositivi di memorizzazione USB tranne l'unità a dischetti USB. Chiudere il coperchio del computer.
4. Ricollegare il computer ed accenderlo. Non appena la spia del monitor diventa verde, premere il tasto **F10** per passare all'utility Computer Setup.
5. In Advanced/PCI devices (Dispositivi avanzati/PCI) disabilitare i controller IDE e SATA. Quando si disabilita il controller SATA, annotare l'IRQ al quale viene assegnato il controller, in quanto lo si dovrà riassegnare in seguito. Confermare le modifiche per uscire dalla procedura di configurazione.

   IRQ SATA: _____
6. Inserire nell'unità a dischetti un dischetto DOS avviabile con FDISK.COM e SYS.COM o FORMAT.COM e accendere il computer per avviare il dischetto DOS.
7. Eseguire FDISK e cancellare eventuali partizioni esistenti sul dispositivo flash media USB. Creare una nuova partizione e segnarla come attiva. Per uscire da FDISK, premere il tasto **Esc**.
8. Se il sistema non si riavvia automaticamente all'uscita da FDISK, premere **Ctrl+Alt+Canc** per riavviarlo dal dischetto DOS.
9. Al prompt A:\ digitare **FORMAT C: /S** e premere **Invio**. FORMAT formatta il dispositivo flash media USB, aggiunge i file di sistema e richiede l'immissione di un'etichetta di volume.
10. Premere **Invio** per non inserire nessuna etichetta o digitarne l'eventuale testo.
11. Spegnere il computer e scollegare il cavo d'alimentazione. Aprire il computer e reinstallare eventuali schede PCI tolte in precedenza. Chiudere il coperchio del computer.
12. Ricollegare il cavo d'alimentazione, togliere il dischetto e riaccendere il computer.
13. Non appena la spia del monitor diventa verde, premere il tasto **F10** per passare all'utility Computer Setup.

14. In Advanced/PCI Devices riabilitare i controller IDE e SATA disabilitati in precedenza. Ricollocare il controller SATA nell'IRQ originale.
15. Salvare le modifiche e uscire. Il computer si avvia con il dispositivo flash media USB come unità C.

La sequenza d'avvio predefinita varia da computer a computer, e può essere modificata nell'utility Computer Setup (F10).

Se si è utilizzata una versione DOS di Windows 9x, è possibile che appaia una schermata con il logo di Windows. Per non visualizzarla aggiungere il file LOGO.SYS vuoto alla directory principale del Drive Key.

Ritornare a "Copia su più computer" a pagina 11.

Pulsante d'accensione a due stati

Con le funzioni ACPI (Advanced Configuration and Power Interface) abilitate in Windows 2000 e Windows XP Professional e Home Edition, il pulsante può funzionare come interruttore di accensione o come interruttore di sospensione. La funzione di sospensione non interrompe completamente l'alimentazione, ma fa entrare il computer in una modalità di consumo energetico minimo. In tal modo è possibile spegnere velocemente il computer senza chiudere le applicazioni e ritornare altrettanto velocemente allo stesso stato operativo senza alcuna perdita di dati.

Per cambiare la configurazione del pulsante di accensione procedere come segue:

1. In Windows 2000, fare clic su **Start** e selezionare **Impostazioni > Pannello di controllo > Opzioni risparmio energia**.

   In Windows XP Professional e Home Edition, fare clic su **Start** e selezionare **Pannello di controllo > Prestazioni e manutenzione > Opzioni risparmio energia**.
2. In **Proprietà – Opzioni risparmio energia** selezionare la scheda **Avanzate**.
3. Nella sezione **Pulsanti di alimentazione** selezionare l'impostazione preferita.

Dopo aver configurato il pulsante di accensione come pulsante di standby, premerlo per portare il sistema ad uno stato di alimentazione ridotta (Sospendi). Premere di nuovo il pulsante per riportare rapidamente il sistema dallo standby allo stato di piena alimentazione. Per interrompere completamente l'alimentazione al sistema, premere e tenere premuto il pulsante di accensione per quattro secondi.

ATTENZIONE: Utilizzare il pulsante di accensione per spegnere il computer unicamente se il sistema non risponde: lo spegnimento del computer senza interazione col sistema operativo può provocare danni al disco fisso o perdita di dati.

Sito World Wide Web

I tecnici HP controllano rigorosamente e mettono a punto il software prodotto da HP e da altri fornitori e sviluppano software di supporto specifici per i sistemi operativi, per garantire prestazioni, compatibilità e affidabilità dei personal computer HP.

Quando si passa a sistemi operativi nuovi o modificati, è importante implementare il software di supporto creato per il sistema operativo. Se si prevede di utilizzare una versione di Microsoft Windows diversa da quella preinstallata, è necessario installare i driver corrispondenti e le utility necessarie per garantire il corretto funzionamento.

HP ha reso più facile il compito di localizzare, accedere, valutare e installare il software di supporto più recente. Scaricare il software da http://www.hp.com/support.

Il sito contiene gli aggiornamenti ai driver, alle utility ed alle immagini ROM aggiornabili mediante flash, occorrenti per eseguire i sistemi operativi Microsoft Windows sui computer HP.

Moduli e collaboratori

Le soluzioni di gestione HP si integrano con altre applicazioni di gestione sistemi e si basano su standard industriali quali:

- Desktop Management Interface (DMI) 2.0
- Tecnologia WON (Wake on LAN)
- ACPI
- SMBIOS
- Supporto Pre-boot Execution (PXE)

Controllo e sicurezza delle risorse

Le funzioni di controllo delle risorse integrate nei PC forniscono dati di controllo sulle principali risorse gestibili con prodotti HP Insight Manager, HP Client Manager o altre applicazioni di gestione sistemi. L'integrazione automatica e perfetta tra le funzioni di controllo delle risorse e questi prodotti consente di scegliere lo strumento di gestione che meglio si adatta al proprio ambiente e che consente di sfruttare al massimo l'investimento in termini di strumenti già esistenti.

HP offre inoltre diverse soluzioni per il controllo dell'accesso ai componenti e ai dati critici del computer. La funzione di sicurezza integrata ProtectTools, se installata, impedisce l'accesso non autorizzato a dati, controlla l'integrità del sistema ed autentica eventuali utenti estranei che tentino di accedervi. Le funzioni di sicurezza come ProtectTools, il sensore e la chiusura Smart Cover, disponibili su alcuni modelli, impediscono l'accesso non autorizzato ai componenti interni del personal computer. Disabilitando le porte parallela, seriale od USB, o disabilitando la funzione d'avvio da supporto rimovibile è possibile proteggere risorse dati preziose. Gli allarmi di modifica alla memoria e quelli trasmessi dal sensore Smart Cover possono essere inoltrati automaticamente alle applicazioni di gestione sistemi per fornire un'efficace segnalazione dei tentativi di manomissione dei componenti.

ProtectTools, il sensore e il dispositivo di chiusura Smart Cover sono disponibili come optional su alcuni sistemi.

Per gestire le impostazioni di sicurezza dei computer HP procedere come di seguito indicato:

- In loco, utilizzando le utility di Computer Setup. Per ulteriori informazioni sull'uso delle utility Computer Setup vedere la *Guida all'utility Computer Setup (F10)* in dotazione al computer.
- A distanza, utilizzare HP Client Manager o System Software Manager. Questo software consente un'installazione sicura e ottimizzata e di controllare le impostazioni di sicurezza con una semplice utility da eseguire dalla riga di comando.

La tabella e le sezioni seguenti si riferiscono alla gestione delle caratteristiche di sicurezza del computer a livello locale tramite le utility di Computer Setup (F10).

Descrizione generale delle funzioni di sicurezza

Funzione	Scopo	Come viene attivata
Removable Media Boot Control (Controllo avvio dispositivi removibili)	Impedisce l'avvio da unità a supporti rimovibili (solo su alcuni modelli).	Dal menu Utility di Computer Setup (F10).
Serial, Parallel, USB, or Infrared Interface Control (Controllo inferfaccia seriale, parallela, USB o infrarossi)	Impedisce il trasferimento di dati tramite le interfacce seriali, parallele, USB (Universal Serial Bus) o a infrarossi.	Dal menu Utility di Computer Setup (F10).
Power-On Password (Password d'accensione)	Impedisce l'uso del computer finché non viene immessa la password. Ciò vale sia per l'avvio iniziale che per le operazioni di riavvio.	Dal menu Utility di Computer Setup (F10).
Setup Password (Password di impostazione)	Impedisce la riconfigurazione del computer (uso delle utility di Computer Setup) finché non viene immessa la password.	Dal menu Utility di Computer Setup (F10).
Embedded Security Device (Dispositivo di sicurezza integrata)	Impedisce l'accesso non autorizzato ai dati tramite crittografia e protezione mediante password. Verifica l'integrità del sistema ed autentica utenti estranei che tentino di accedervi.	Dal menu Utility di Computer Setup (F10).
DriveLock	Impedisce l'accesso non autorizzato ai dati su unità disco rigido MultiBay. Questa funzione è disponibile solo su alcuni modelli.	Dal menu Utility di Computer Setup (F10).

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*. Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Funzione	Scopo	Come viene attivata
Smart Cover Sensor (Sensore Smart Cover)	Indica che il coperchio o il pannello laterale del computer sono stati rimossi. È possibile impostarlo in modo che venga richiesta la password di configurazione per il riavvio del computer, dopo la rimozione del coperchio o del pannello laterale. Per ulteriori informazioni su questa funzione, consultare la *Guida di riferimento hardware* sul CD *Documentation Library*. Questa funzione è disponibile solo su alcuni modelli.	Dal menu Utility di Computer Setup (F10).
Master Boot Record Security (Sicurezza MBR (Master Boot Record))	Serve per impedire che il Master Boot Record del disco d'avvio venga modificato inavvertitamente o dolosamente e per ripristinare l'ultimo MBR valido.	Dal menu Utility di Computer Setup (F10).
Memory Change Alerts (Allarmi di variazione memoria)	Rileva l'aggiunta, lo spostamento o la rimozione di moduli di memoria, informandone l'utente finale e l'amministratore del sistema.	Per informazioni sull'abilitazione degli allarmi di modifica alla memoria consultare la guida in linea *Intelligent Manageability Guide*.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*. Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Descrizione generale delle funzioni di sicurezza *(Continuazione)*

Funzione	Scopo	Come viene attivata
Ownership Tag (Contrassegno proprietà)	Durante l'avvio del sistema (protetto da password di configurazione), visualizza le informazioni relative alla proprietà, come definite dall'amministratore del sistema.	Dal menu Utility di Computer Setup (F10).
Cable Lock Provision (Predisposizione per chiusura con cavo)	Impedisce l'accesso all'interno del computer per impedire modifiche non autorizzate della configurazione o la rimozione di componenti. È possibile utilizzarla anche per fissare il computer ad un oggetto immobile, in modo da impedirne il furto.	Utilizzare una chiusura con cavo per assicurare il computer ad un oggetto fisso.
Security Loop Provsion (Chiusura di sicurezza)	Impedisce l'accesso all'interno del computer per impedire modifiche non autorizzate della configurazione o la rimozione di componenti.	Installare un lucchetto nella chiusura di sicurezza per impedire modifiche non autorizzate della configurazione o la rimozione di componenti.

✎ Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*. Il supporto delle funzioni di sicurezza può variare a seconda della configurazione del computer.

Sicurezza tramite password

La password di accensione impedisce l'utilizzo non autorizzato del computer richiedendo l'immissione di una password per accedere alle applicazioni o ai dati ogni volta che il computer viene acceso o riavviato. La password di impostazione impedisce in modo specifico l'accesso non autorizzato a Computer Setup, e può anche essere utilizzata per escludere la password di accensione. Ciò significa che, quando viene richiesta la password di accensione, è possibile accedere al computer anche immettendo la password di configurazione.

È possibile impostare un'unica password per l'intera rete, al fine di consentire all'amministratore della rete di accedere a tutti i sistemi della rete per eseguire le operazioni di manutenzione senza conoscerne la password di accensione, nel caso ne sia stata attivata una.

Impostazione di una password di impostazione tramite Computer Setup

Se il sistema è dotato di un dispositivo di sicurezza integrato consultare "Sicurezza integrata" a pagina 29.

Se si imposta una password di impostazione tramite Computer Setup, si impedisce la riconfigurazione del computer (uso dell'utility di Computer Setup (F10)) finché non viene immessa la password.

1. Accendere o riavviare il computer. Se si è in Windows, scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Selezionare **Sicurezza**, quindi **Password di configurazione** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Immissione della password di accensione con Computer Setup

Impostando una password di accensione in Computer Setup si impedisce l'accesso al computer all'accensione, finché non viene immessa la password. Se è stata impostata la password di accensione, Computer Setup presenta le opzioni disponibili (Password Options) nel menu Security (Sicurezza). Tra le opzioni della password figura Password Prompt on Warm Boot (Richiesta password al riavvio). Se l'opzione Password Prompt on Warm Boot è abilitata, la password dev'essere immessa ogni volta che il computer viene riavviato.

1. Accendere o riavviare il computer. Se si è in Windows, scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde, premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Selezionare **Sicurezza**, quindi **Password di accensione** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Immissione della password di accensione

Per immettere la password di accensione procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows, scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Quando viene visualizzata sul monitor l'icona della chiave, digitare la password attuale e premere **Invio**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

Se si immette la password in modo errato, viene visualizzata un'icona di chiave spezzata. Tentare di nuovo. Dopo tre tentativi falliti, è necessario spegnere il computer e riaccenderlo, prima di poter continuare.

Immissione di una password di impostazione

Se il sistema è dotato di un dispositivo di sicurezza integrato, consultare "Sicurezza integrata" a pagina 29.

Se sul PC è stata impostata la password di configurazione, ne viene richiesta l'immissione ogni volta che viene eseguito Computer Setup.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde, premere il tasto **F10**.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Quando viene visualizzata sul monitor l'icona della chiave, digitare la password di impostazione e premere il tasto **Invio**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

Se si immette la password in modo errato, viene visualizzata un'icona di chiave spezzata. Tentare di nuovo. Dopo tre tentativi falliti, è necessario spegnere il computer e riaccenderlo, prima di poter continuare.

Modifica delle password di accensione e di impostazione

Se il sistema è dotato di un dispositivo di sicurezza integrato consultare "Sicurezza integrata" a pagina 29.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**. Per cambiare la password di impostazione, eseguire **Computer Setup**.
2. Quando viene visualizzata l'icona della chiave, digitare la password, una barra (/) o un carattere delimitatore alternativo, la nuova password, un'altra barra (/) o un carattere delimitatore alternativo e ancora la nuova password, come di seguito precisato:
   password attuale/nuova password/nuova password

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

3. Premere **Invio**.

La nuova password sarà in vigore a partire dalla prossima volta che si accende il computer.

Per informazioni sui caratteri delimitatori alternativi, consultare "Caratteri delimitatori delle tastiere nazionali" a pagina 28.
È possibile modificare la password di accensione e di impostazione anche utilizzando le opzioni di sicurezza di Computer Setup.

Cancellazione delle password di accensione e di impostazione

Se il sistema è dotato di un dispositivo di sicurezza integrato consultare "Sicurezza integrata" a pagina 29.

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**. Per cancellare la password di impostazione, eseguire **Computer Setup**.
2. Quando viene visualizzata l'icona della chiave, digitare la password attuale seguita da una barra (/) o da un carattere delimitatore alternativo, come qui illustrato:
   password attuale/
3. Premere **Invio**.

Per informazioni sui caratteri delimitatori alternativi consultare "Caratteri delimitatori delle tastiere nazionali". È possibile modificare la password di accensione e di impostazione anche utilizzando le opzioni di sicurezza di Computer Setup.

Caratteri delimitatori delle tastiere nazionali

Ciascuna tastiera è concepita per soddisfare i requisiti specifici dei singoli paesi. La sintassi e i tasti per la modifica o la cancellazione delle password dipendono dalla tastiera utilizzata.

Caratteri delimitatori delle tastiere nazionali

Araba	/	Greca	-	Russa	/
Belga	=	Ebraica	.	Slovacca	-
BHCSY*	-	Ungherese	-	Spagnola	-
Brasiliana	/	Italiana	-	Svedese/Finnica	/
Cinese	/	Giapponese	/	Svizzera	-
Ceca	-	Coreana	/	Taiwanese	/
Danese	-	Latino-americana	-	Tailandese	/
Francese	!	Norvegese	-	Turca	.
Canadese francofona	é	Polacca	-	Inglese del RU	/
Tedesca	-	Portoghese	-	Inglese degli USA	/

* Per Bosnia-Erzegovina, Croazia, Slovenia e Iugoslavia

Annullamento password

Se si dimentica la password, non è possibile accedere al computer. Per le istruzioni su come eliminare le password, consultare la *Guida alla soluzione dei problemi*.

Se il sistema è dotato di un dispositivo di sicurezza integrato consultare "Sicurezza integrata."

Sicurezza integrata

La funzione di sicurezza integrata ProtectTools abbina crittografia e protezione mediante password per fornire la massima sicurezza per la crittografia di file/cartelle EFS (Embedded File System) e rendere sicure le trasmissioni di posta elettronica con Microsoft Outlook e Outlook Express. ProtectTools è disponibile su determinati business desktop come opzione CTO (Configured-To-Order) ed è destinato a clienti HP per i quali la sicurezza dei dati è fondamentale e l'eventuale accesso non autorizzato ai dati rappresentano un rischio molto maggiore della perdita dei dati. ProtectTools utilizza quattro password:

- (F10) Setup: per accedere all'utility Computer Setup (F10) ed abilitare/disabilitare ProtectTools
- Take Ownership: dev'essere impostata ed utilizzata dall'amministratore di sistema, il quale autorizza gli utenti ed imposta i parametri di sicurezza
- Emergency Recovery Token: dev'essere impostata dall'amministratore di sistema, consente il recupero in caso di guasto del computer o del chip ProtectTools
- Basic User: dev'essere impostata ed utilizzata dall'utente finale.

Se si perde la password dell'utente finale non sarà possibile recuperare i dati crittografati. Pertanto, ProtectTools risulta maggiormente indicato quando i dati contenuti sul disco fisso vengono replicati su un sistema informatico aziendale o quando ne viene effettuato il backup su base regolare.

La sicurezza integrata ProtectTools è un chip di sicurezza compatibile TCPA 1.1 installato in via opzionale sulla scheda di sistema di determinati business desktop. Ogni chip ProtectTools Embedded Security è univoco ed è legato ad un determinato computer. Ogni chip esegue processi di sicurezza fondamentali indipendentemente da altri componenti del computer (processore, memoria o sistema operativo).

Un computer abilitato ProtectTools Embedded Security implementa e migliora le funzioni di sicurezza presenti in Microsoft Windows 2000 o Windows XP Professional o Home Edition. Ad esempio, mentre il sistema operativo può crittografare file e cartelle locali sulla base di un EFS, la funzione ProtectTools prevede un ulteriore livello di sicurezza ottenuto mediante codici crittografici dalla root key della piattaforma (memorizzata su chip). Questo processo viene detto "wrapping" dei codici di crittografia. ProtectTools non impedisce l'accesso alla rete a computer senza ProtectTools.

Le funzioni fondamentali della sicurezza ProtectTools sono:

- Autenticazione della piattaforma
- Memorizzazione protetta
- Integrità dei dati

ATTENZIONE: Tutela delle password. **Senza password non è possibile accedere ai dati crittografati né recuperarli**.

Impostazione delle password

Configurazione

Con l'utility Computer Setup F10 è possibile creare una password di impostazione ed abilitare il dispositivo di sicurezza integrata.

1. Non appena la spia del monitor diventa verde premere il tasto **F10**.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

2. Con i tasti freccia in su/in giù selezionare la lingua e premere **Invio**.
3. Con i tasti freccia sinistra o destra spostarsi nella scheda **Security (Sicurezza)** ed utilizzare i tasti freccia in su/in giù per passare a **Setup Password (Password setup)**. Premere **Invio**.
4. Digitare una password e confermarla. Premere **F10** per accettare la password.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

5. Con i tasti freccia in su/in giù spostarsi su **Embedded Security Device (Dispositivo di sicurezza integrata)**. Premere **Invio**.
6. Se la selezione nella finestra di dialogo è disabilitata (**Embedded Security Device – Disable**) utilizzare i tasti freccia sinistra o destra per abilitarla (**Embedded Security Device – Enable**). Premere **F10** per accettare la modifica.

ATTENZIONE: Se si seleziona **Reset to Factory Settings – Reset (Ripristina le impostazioni predefinite: Ripristina)**, tutti i codici vengono cancellati e i dati crittografati non saranno recuperabili *a meno che* non sia stato eseguito il backup dei codici (vedere "Take Ownership ed Emergency Recovery Token"). Selezionare solo **Reset (Ripristina)** quando la procedura lo richiede per poter recuperare i dati crittografati (vedere "Recupero dei dati crittografati" a pagina 34).

7. Con i tasti freccia sinistra o destra, spostarsi su **File**. Con i tasti freccia in su/in giù spostarsi su **Save Changes and Exit** (**Salva modifiche ed Esci**). Premere **Invio**, quindi **F10** per confermare.

Take Ownership ed Emergency Recovery Token

La password Take Ownership è necessaria per abilitare o disabilitare la piattaforma di sicurezza e per autorizzare gli utenti. Se il dispositivo di sicurezza integrata non funziona, il meccanismo Emergency Recovery consente di autorizzare gli utenti ed accedere ai dati.

1. In Windows XP Professional o Home Edition, fare clic su **Start > Tutti i programmi > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (**Procedura guidata di inizializzazione sicurezza integrata**).

   In Windows 2000 fare clic su **Start > Programmi > HP ProtectTools Embedded Security Tools (Strumenti di sicurezza integrata HP ProtectTools) > Embedded Security Initialization Wizard**.
2. Fare clic su **Next (Avanti)**.
3. Digitare una password Take Ownership, confermarla e fare clic su **Next**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

4. Fare clic su **Next** per accettare la posizione di archiviazione predefinita.
5. Digitare una password Emergency Recovery Token, confermarla e fare clic su **Next**.
6. Inserire un dischetto su cui memorizzare il codice Emergency Recovery Token. Fare clic su **Browse (Sfoglia)** e selezionare il dischetto.

ATTENZIONE: L'Emergency Recovery Token Key viene utilizzato per recuperare dati crittografati nel caso di un guasto al computer o al chip di sicurezza integrata. **Senza il codice non è possibile recuperare i dati**. (Ai dati non è possibile accedere senza la password Basic User.) Riporre il dischetto in un luogo sicuro.

7. Fare clic su **Save (Salva)** per accettare la posizione e il nome del file predefiniti, quindi fare clic su **Next**.
8. Fare clic su **Next** per confermare le impostazioni prima che la piattaforma di sicurezza sia inizializzata.

Può apparire un messaggio che avverte che le funzioni di sicurezza integrata non sono inizializzate. Non fare clic sul messaggio; il problema verrà risolto più avanti nella procedura e il messaggio sparirà dopo pochi secondi.

9. Fare clic su **Next** per bypassare le impostazioni di configurazione locali.
10. Verificare che la casella di controllo di avvio della procedura guidata (Start Embedded Security User Initialization Wizard) sia selezionata e fare clic su **Finish (Fine)**.

La procedura guidata di inizializzazione utente si avvia automaticamente.

Basic User

In fase di inizializzazione utente viene creata la password Basic User, necessaria per inserire ed accedere ai dati crittografati.

ATTENZIONE: Protezione della password Basic User. **Senza password non è possibile accedere ai dati crittografati né recuperarli**.

1. Se la procedura guidata di inizializzazione utente non è avviata:

   In Windows XP Professional o Home Edition, fare clic su **Start > Tutti i programmi > HP ProtectTools Embedded Security Tools > User Initialization Wizard (Procedura guidata inizializzazione utente)**.

   In Windows 2000 fare clic su **Start > Programmi > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

2. Fare clic su **Next**.
3. Digitare una password Basic User Key, confermarla e fare clic su **Next**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

4. Fare clic su **Next** per confermare le impostazioni.
5. Selezionare le idonee funzioni di sicurezza e fare clic su **Next**.
6. Fare clic su un client di posta elettronica per selezionarlo e fare clic su **Next**.
7. Fare clic su **Next** per applicare il certificato di crittografia.
8. Fare clic su **Next** per confermare le impostazioni.
9. Fare clic su **Finish**.
10. Riavviare il computer.

Recupero dei dati crittografati

Per recuperare i dati dopo aver sostituito il chip ProtectTools è necessario possedere:

- SPEmRecToken.xml: il codice Emergency Recovery Token
- SPEmRecArchive.xml: cartella nascosta, posizione predefinita: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Password ProtectTools
  - Setup (di impostazione)
  - Take Ownership
  - Emergency Recovery Token
  - Basic User

1. Riavviare il computer.
2. Non appena la spia del monitor diventa verde premere il tasto **F10**.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Digitare la password di impostazione e premere **Invio**.
4. Con i tasti freccia in su/in giù selezionare la lingua e premere **Invio**.
5. Con i tasti freccia sinistra o destra spostarsi nella scheda **Security** ed utilizzare i tasti freccia in su/in giù per passare a **Embedded Security Device**. Premere **Invio**.
6. Se è disponibile la sola opzione di dispositivo disabilitato (**Embedded Security Device – Disable**):
   a. Con i tasti freccia sinistra o destra abilitare il dispositivo (**Embedded Security Device – Enable**). Premere **F10** per accettare la modifica.
   b. Con i tasti freccia sinistra o destra spostarsi su **File**. Con i tasti freccia in su/in giù spostarsi su **Save Changes and Exit**. Premere **Invio**, quindi **F10** per confermare.
   c. Passare al punto 1.

   Se sono disponibili due opzioni passare al punto 7.

7. Con i tasti freccia in su/in giù spostarsi su **Reset to Factory Settings – Do Not Reset (Ripristina le impostazioni predefinite: Ripristina)**. Premere una volta il tasto freccia sinistra o destra.

   Viene visualizzato un messaggio che segnala che: salvando le modifiche all'uscita, l'esecuzione di questa azione riporterà il dispositivo di sicurezza integrata alle impostazioni predefinite. Premere un tasto qualsiasi per continuare.

   Premere **Invio**.

8. L'opzione appare modificata in **Reset to Factory Settings – Reset**. Premere **F10** per accettare la modifica.
9. Con i tasti freccia sinistra o destra spostarsi su **File**. Con i tasti freccia in su/in giù spostarsi su **Save Changes and Exit (Salva modifiche ed Esci)**. Premere **Invio**, quindi **F10** per confermare.
10. Riavviare il computer.
11. Non appena la spia del monitor diventa verde, premere il tasto **F10**.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

12. Digitare la password di impostazione e premere **Invio**.
13. Con i tasti freccia in su/in giù selezionare la lingua e premere **Invio.**
14. Con i tasti freccia sinistra o destra spostarsi nella scheda **Security** ed utilizzare i tasti freccia in su/in giù per passare a **Embedded Security Device**. Premere **Invio**.
15. Se la selezione nella finestra di dialogo è disabilitata (**Embedded Security Device – Disable**) utilizzare i tasti freccia sinistra o destra per abilitarla (**Embedded Security Device – Enable**). Premere **F10**.
16. Con i tasti freccia sinistra o destra spostarsi su **File**. Con i tasti freccia in su/in giù spostarsi su **Save Changes and Exit**. Premere **Invio**, quindi **F10** per confermare.

17. Una volta avviato Windows:

    In Windows XP Professional o Home Edition, fare clic su **Start > Tutti i programmi > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

    In Windows 2000 fare clic su **Start > Programmi > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

18. Fare clic su **Next**.
19. Digitare una password Take Ownership e confermarla. Fare clic su **Next**.

Digitare la password con attenzione; per motivi di sicurezza, i caratteri digitati non vengono visualizzati sullo schermo.

20. Verificare che sia selezionata l'opzione Create a new recovery archive (Crea un nuovo archivio di recupero). In **Recovery archive location** (Posizione archivio di recupero) fare clic su **Browse**.
21. Non accettare il nome del file predefinito. Digitarne uno nuovo per evitare di sostituire il file originale.
22. Fare clic su **Save** e su **Next**.
23. Digitare una password Emergency Recovery Token, confermarla e fare clic su **Next**.
24. Inserire un dischetto su cui memorizzare il codice Emergency Recovery Token. Fare clic su **Browse (Sfoglia)** e selezionare il dischetto.
25. Non accettare il nome del Key predefinito. Digitarne uno nuovo per evitare di sostituire quello originale.
26. Fare clic su **Save** e su **Next**.
27. Fare clic su **Next** per confermare le impostazioni prima che la piattaforma di sicurezza sia inizializzata.

Viene visualizzato un messaggio che segnala che non è possibile caricare il Basic User Key. Non fare clic sul messaggio; il problema verrà risolto più avanti nella procedura e il messaggio sparirà dopo pochi secondi.

28. Fare clic su **Next** per bypassare le impostazioni di configurazione locali.
29. Fare clic per deselezionare la casella di controllo di avvio della procedura guidata (**Start Embedded Security User Initialization Wizard**). Fare clic su **Finish**.
30. Fare clic con il pulsante destro del mouse sull'icona ProtectTools nella barra degli strumenti e su **Initialize Embedded Security restoration (Inizializza ripristino sicurezza integrata)**.

    per avviare la procedura guidata corrispondente.
31. Fare clic su **Next**.
32. Inserire il dischetto sul quale è memorizzato l'Emergency Recovery Token Key originale. Fare clic su **Browse**, individuare e fare doppio clic sul Token per inserire il nome nel campo. Il nome predefinito è A:\SPEmRecToken.xml.
33. Digitare la password Token originale e fare clic su **Next**.
34. Fare clic su **Browse**, individuare e fare doppio clic sull'archivio di recupero per inserire il nome nel campo. Il nome predefinito è C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Fare clic su **Next**.
36. Fare clic sulla macchina da ripristinare e su **Next**.
37. Fare clic su **Next** per confermare le impostazioni.
38. Se la procedura guidata comunica che la piattaforma di sicurezza è stata ripristinata passare al punto 39.

    Se invece l'operazione non è riuscita, ritornare al punto 10. Verificare con attenzione password, posizione e nome del token, posizione e nome dell'archivio.
39. Fare clic su Finish.
40. In Windows XP Professional o Home Edition, fare clic su **Start > Tutti i programmi > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

    In Windows 2000 fare clic su **Start > Programmi > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
41. Fare clic su **Next**.
42. Fare clic su **Recover your basic user key (Recupera Basic User Key)** e su **Next**.

43. Selezionare un utente, digitare la password Basic User Key originale e fare clic su **Next**.
44. Fare clic su **Next** per confermare le impostazioni ed accettare la posizione predefinita dei dati di recupero.

Le fasi da 45 a 49 reinstalla la configurazione Basic User originale.

45. Selezionare le idonee funzioni di sicurezza e fare clic su **Next**.
46. Fare clic su un client di posta elettronica per selezionarlo e fare clic su **Next**.
47. Fare clic sul certificato di crittografia e su **Next** per applicarlo.
48. Fare clic su **Next** per confermare le impostazioni.
49. Fare clic su **Finish**.
50. Riavviare il computer.

ATTENZIONE: Protezione della password Basic User. **Senza password non è possibile accedere ai dati crittografati né recuperarli**.

DriveLock

DriveLock è una funzione di sicurezza di standard industriale che impedisce l'accesso non autorizzato ai dati memorizzati su dischi MultiBay. DriveLock è stato implementato come estensione di Computer Setup ed è disponibile quando vengono rilevate unità dischi rigidi compatibili con DriveLock.

DriveLock è destinato a clienti HP per i quali la sicurezza dei dati è fondamentale. Per tali clienti il costo del disco fisso e la perdita dei dati ivi memorizzati hanno un'importanza secondaria rispetto al danno provocato da un accesso non autorizzato al contenuto. Per bilanciare questo livello di sicurezza con l'esigenza pratica di consentire l'accesso in caso di smarrimento della password, l'implementazione HP di DriveLock utilizza uno schema di sicurezza a doppia password: una dev'essere impostata ed utilizzata da un amministratore di sistema, mentre l'altra viene normalmente impostata ed utilizzata dall'utente finale. Non sono previsti accorgimenti per sbloccare il disco se vengono smarrite entrambe le password. Pertanto, DriveLock risulta maggiormente indicato quando i dati contenuti sul disco fisso vengono replicati su un sistema informatico aziendale o quando ne viene effettuato il backup su base regolare.

Se entrambe le password di DriveLock vengono smarrite, il disco fisso è reso inutilizzabile. Per gli utenti che non rispondono ai criteri sopra delineati questo può essere un rischio inaccettabile. Per quelli, invece, che rispondono a tali criteri, il rischio può essere tollerabile, data la natura dei dati memorizzati sul disco.

Uso di DriveLock

L'opzione DriveLock è disponibile nel menu Security (Sicurezza) di Computer Setup. L'utente ha la possibilità di impostare la password principale o di abilitare DriveLock. Per abilitare DriveLock dev'essere specificata una password utente. Dal momento che la configurazione iniziale di DriveLock viene normalmente eseguita da un amministratore di sistema, dev'essere prima di tutto impostata la password principale. HP invita gli amministratori di sistema ad impostare una password principale sia che prevedano di abilitare DriveLock, sia che prevedano di non abilitarlo. In tal modo gli amministratori avranno la possibilità di modificare le impostazioni di DriveLock se si deciderà di bloccare il disco in un secondo tempo. Una volta impostata la password principale l'amministratore di sistema potrà abilitare o meno DriveLock.

Se è presente un disco fisso bloccato, durante il POST chiede la password per sbloccarlo. Se viene impostata una password di accensione e la stessa coincide con quella dell'utente della periferica, durante il POST non viene richiesto all'utente di reimmettere la password. Altrimenti, all'utente viene richiesto di immettere la password per accedere a DriveLock. È possibile utilizzare a tal fine la password principale o quella dell'utente. Gli utenti hanno a disposizione due tentativi per immettere la password corretta. Se entrambi non riescono, il POST prosegue ma il disco resta inaccessibile.

Applicazioni di DriveLock

La condizione più indicata per la funzione di sicurezza DriveLock è in ambito aziendale, quando un amministratore di sistema fornisce agli utenti dischi fissi MultiBay da utilizzare in alcuni computer desktop. L'amministratore di sistema è responsabile della configurazione del disco fisso MultiBay che comporta, tra l'altro, l'impostazione della password principale di DriveLock. Se l'utente dimentica la sua password o la macchina passa ad un altro impiegato, è possibile utilizzare la password principale per cambiare la password utente e accedere nuovamente al disco.

HP consiglia agli amministratori dei sistemi aziendali che decidono di abilitare DriveLock di definire una politica aziendale per l'impostazione e il mantenimento delle password principali. Questa operazione ha lo scopo d'impedire che un dipendente, prima di lasciare l'azienda, imposti intenzionalmente o casualmente entrambe le password di DriveLock. In una simile eventualità il disco fisso non potrebbe più essere utilizzato e dovrebbe essere sostituito. Analogamente, non impostando la password principale gli amministratori di sistema potrebbero vedersi impedito l'accesso al disco per eseguire i controlli di routine del software non autorizzato, altre funzioni di controllo risorse e di supporto.

Per utenti con esigenze di sicurezza meno rigide, HP sconsiglia di abilitare DriveLock. Appartengono a questa tipologia singoli utenti ed utenti che conservano dati non importanti sui dischi fissi. Per questi utenti il rischio di perdere il disco in caso di smarrimento di entrambe le password è decisamente superiore al valore dei dati che DriveLock dovrebbe proteggere. L'accesso a Computer Setup e a DriveLock può essere limitato tramite la password di impostazione. Specificando la password di impostazione senza comunicarla agli utenti, gli amministratori di sistema possono impedire loro di abilitare DriveLock.

Sensore Smart Cover

Il sensore Smart Cover, disponibile su alcuni modelli, è una combinazione di tecnologia hardware e software in grado di segnalare se il coperchio o il pannello laterale del computer sono stati tolti. Esistono tre livelli di protezione, come risulta dalla seguente tabella:

Livelli di protezione del sensore Smart Cover

Livello	Impostazione	Descrizione
Livello 0	Disabled (Disattivato)	Il sensore Smart Cover è disattivato (impostazione predefinita).
Livello 1	Notify User (Notifica all'utente)	Quando il computer viene riavviato, sullo schermo viene visualizzato un messaggio che avverte che il coperchio o il pannello laterale del computer sono stati rimossi.
Livello 2	Setup Password (Password di impostazione)	Quando il computer viene riavviato, sullo schermo viene visualizzato un messaggio che avverte che il coperchio o il pannello laterale del computer sono stati rimossi. Per continuare, è necessario immettere la password di impostazione.

✎ Le impostazioni possono essere modificate tramite Computer Setup. Per ulteriori informazioni su Computer Setup vedere la *Guida all'utility Computer Setup (F10)*.

Impostazione del livello di protezione del sensore Smart Cover

Per impostare il livello di protezione del sensore Smart Cover procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Selezionare **Security (Sicurezza)**, quindi **Smart Cover** e seguire le istruzioni a video.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Chiusura Smart Cover

La chiusura Smart Cover è un dispositivo di blocco a controllo informatizzato, presente su alcuni computer HP. Esso impedisce l'accesso non autorizzato ai componenti interni. Alla consegna, i computer hanno la chiusura Smart Cover sbloccata.

ATTENZIONE: Per garantire la massima sicurezza del blocco del coperchio, è bene stabilire una password di impostazione. La password impedisce l'accesso non autorizzato all'utility Computer Setup.

La chiusura Smart Cover è disponibile come optional su determinati modelli.

Blocco della chiusura Smart Cover

Per attivare e bloccare la chiusura Smart Cover procedere come di seguito indicato:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Selezionare **Security (Sicurezza)**, quindi **Smart Cover** e l'opzione **Bloccata**.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Disattivazione del blocco di Smart Cover

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Selezionare **Security (Sicurezza) > Smart Cover > Unlocked (Sbloccata)**.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Uso della chiave FailSafe Smart Cover

Se la chiusura Smart Cover è abilitata e non è possibile immettere la password per disabilitarla, per aprire il coperchio del computer è necessaria la chiave Failsafe di Smart Cover. La chiave è necessaria in tutte le seguenti circostanze:

- Mancanza di corrente
- Guasto all'avvio
- Guasto dei componenti del PC (ad esempio, processore o alimentatore)
- Password dimenticata

ATTENZIONE: La chiave FailSafe di Smart Cover è uno strumento speciale disponibile presso HP. Per sicurezza si consiglia di ordinare la chiave prima che sia necessario utilizzarla presso un venditore o un centro assistenza autorizzati.

È possibile procurarsi la chiave FailSafe in diversi modi:

- Contattare un rivenditore o un centro assistenza autorizzati HP.
- Chiamare il numero di telefono appropriato, riportato nella garanzia.

Per ulteriori informazioni sull'utilizzo della chiave FailSafe di Smart Cover consultare la *Guida di riferimento hardware.*

Master Boot Record Security (Sicurezza MBR (Master Boot Record))

Il Master Boot Record (MBR) contiene le informazioni necessarie per l'avvio da un disco e l'accesso ai dati ivi memorizzati. La sicurezza del Master Boot Record serve per impedire modifiche involontarie o dolose al MBR, come quelle provocate da alcuni virus o dall'uso non corretto di alcune utility. Inoltre essa consente di ripristinare l'ultimo MBR valido nel caso in cui, in fase di riavvio del sistema, vengano rilevate modifiche al MBR.

Per abilitare la sicurezza MBR procedere come segue:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema**.
2. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Selezionare **Security (Sicurezza) > Master Boot Record Security (Sicurezza MBR) > Enabled (Abilitata)**.
4. Selezionare **Security (Sicurezza) > Save Boot Record (Salva MBR)**.
5. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Quando la sicurezza MBR è abilitata, il BIOS impedisce qualsiasi modifica al MBR del disco avviabile corrente in MS-DOS o in Modalità provvisoria di Windows.

La maggior parte dei sistemi operativi controlla l'accesso al MBR del disco avviabile corrente; il BIOS non è in grado d'impedire che vengano apportate modifiche quando il sistema operativo è in funzione.

Ogni volta che il computer viene alimentato o riavviato, il BIOS confronta il MBR del disco d'avvio corrente con quello memorizzato in precedenza. Se vengono rilevate modifiche e se il disco avviabile corrente è lo stesso da cui è stato memorizzato il MBR, viene visualizzato il seguente messaggio:

1999 – Master Boot Record has changed (Il MBR è cambiato).

Premere un tasto per accedere a Computer Setup per configurare la sicurezza MBR.

Una volta in Computer Setup procedere come segue:

- Salvare il MBR del disco avviabile corrente;
- Ripristinare il MBR precedentemente memorizzato; oppure
- Disabilitare la funzione di sicurezza MBR.

È necessario conoscere l'eventuale password di configurazione.

Se vengono rilevate modifiche e se il disco avviabile corrente **non** è lo stesso da cui è stato memorizzato il MBR viene visualizzato il seguente messaggio:

2000 – Master Boot Record Hard Drive has changed (Il disco fisso con il MBR è cambiato).

Premere un tasto per accedere a Computer Setup per configurare la sicurezza MBR.

Una volta in Computer Setup procedere come segue:

- Salvare il MBR del disco avviabile corrente; oppure
- Disabilitare la funzione di sicurezza MBR.

È necessario conoscere l'eventuale password di configurazione.

Nell'improbabile eventualità che il MBR precedentemente salvato si sia danneggiato viene visualizzato il seguente messaggio:

1998 – Master Boot Record has been lost (Il MBR è danneggiato).

Premere un tasto per accedere a Computer Setup per configurare la sicurezza MBR.

Una volta in Computer Setup procedere come segue:

- Salvare il MBR del disco avviabile corrente; oppure
- Disabilitare la funzione di sicurezza MBR.

È necessario conoscere l'eventuale password di configurazione.

Partizionamento e formattazione del disco avviabile corrente

Verificare che la sicurezza MBR sia disabilitata prima di modificare la partizione o prima di formattare il disco avviabile corrente. Alcune utility disco (FDISK e FORMAT) cercano di aggiornare il MBR. Se la sicurezza MBR è abilitata, quando si cambia la partizione o si formatta il disco è possibile che vengano visualizzati messaggi d'errore dall'utility o un avvertimento relativo alla sicurezza MBR in occasione del successivo riavvio del computer. Per disabilitare la sicurezza MBR procedere come segue:

1. Accendere o riavviare il computer. Se si è in Windows scegliere **Start/Avvio > Chiudi sessione > Riavvia il sistema.**
2. Non appena la spia del monitor diventa verde premere il tasto **F10**. Se necessario, premere **Invio** per saltare la schermata del titolo.

Se al momento opportuno non viene premuto il tasto **F10**, per accedere all'utility è necessario spegnere e riaccendere il computer e premere di nuovo **F10**.

3. Selezionare **Security (Sicurezza) > Master Boot Record Security (Sicurezza MBR) > Disabled (Disabilitata)**.
4. Prima di uscire scegliere **File > Salva modifiche** ed **Esci**.

Predisposizione per chiusura con cavo

Sul retro del computer è presente la predisposizione per la chiusura con cavo in modo da bloccare fisicamente il computer al piano di lavoro.

Per le istruzioni consultare la *Guida di riferimento hardware* nel CD *Documentation Library.*

Tecnologia per l'identificazione delle impronte digitali

Eliminando la necessità di immettere le password utente, la tecnologia per il riconoscimento delle impronte digitali di HP migliora la sicurezza della rete, semplificando il processo di accesso e riducendo i costi associati alla gestione delle reti aziendali. Grazie al prezzo accessibile, la funzione non è più appannaggio esclusivo delle organizzazioni high-tech con esigenze di sicurezza elevate.

Il supporto per la tecnologia d'identificazione delle impronte digitali varia da modello a modello.

Per ulteriori informazioni consultare:

http://h18000.www1.hp.com/solutions/security.

Notifica guasti e ripristino

Le funzioni di notifica guasti e ripristino combinano hardware innovativo e tecnologia software al fine di prevenire la perdita di dati critici e ridurre al minimo i periodi di inattività non programmati.

Quando si verifica un guasto, il computer visualizza un messaggio di avviso locale che contiene una descrizione del guasto e le procedure consigliate. Tramite HP Client Manager, è possibile visualizzare lo stato attuale di integrità del sistema. Se è collegato ad una rete gestita da un prodotto HP Insight Manager, HP Client Manager o da altre applicazioni di gestione sistemi, il computer invia anche un avviso di guasto all'applicazione di gestione della rete.

Drive Protection System (DPS)

Il Drive Protection System (DPS) è uno strumento di diagnostica incorporato nei dischi fissi installati su alcuni computer HP, Il DPS è stato progettato per consentire la diagnosi di problemi che potrebbero provocare la sostituzione di unità disco rigido non in garanzia.

In fase di produzione dei PC HP, i dischi fissi installati vengono collaudati uno per uno tramite DPS ed in essi viene registrato un record permanente di dati chiave. Ogni volta che viene eseguito il DPS, gli esiti del test vengono scritti sull'unità disco rigido. Il fornitore di servizi potrà servirsi di queste informazioni per diagnosticare le condizioni che hanno indotto l'utente ad eseguire il software DPS. Per le istruzioni sull'uso del DPS consultare la *Guida alla soluzione dei problemi*.

Alimentatore protetto contro gli sbalzi di tensione

Un alimentatore integrato protetto contro gli sbalzi di tensione garantisce maggiore affidabilità in presenza di instabilità nell'alimentazione. L'alimentatore è concepito per tollerare sbalzi di tensione fino a 2000 volt, senza esporre il sistema periodi di inattività o perdita di dati.

Sensore termico

Il sensore termico è una funzione hardware e software che controlla la temperatura interna del computer. Quando la temperatura supera i valori normali, questa funzione visualizza un messaggio di allarme che consente di intervenire prima che vengano danneggiati i componenti interni o che si verifichi una perdita di dati.

Indice Analitico

A

accesso al computer, controllo 20
ActiveUpdate 6
aggiornamento della ROM 6
alimentatore protetto contro gli sbalzi di tensione 49
Altiris 4
Altiris PC Transplant Pro 5
annullamento password 29
attenzione
    protezione ROM 6
avvertenze
    chiave FailSafe 44
    sicurezza chiusura coperchio 42

B

blocco della chiusura Smart Cover 43

C

cancellazione password 28
caratteri delimitatori tabella 28
caratteri delimitatori tastiere nazionali 28
chiave FailSafe
    avvertenza 44
    ordinazione 44
chiave FailSafe di Smart Cover, ordinazione 44
chiusura Smart Cover 42
    blocco 43
    sblocco 43
configurazione
    iniziale 2
configurazione iniziale 2
configurazione pulsante di accensione 18
controllo accesso al computer 20
controllo risorse 20

D

dischi, clonazione 2
disco avviabile, informazioni importanti 47
DiskOnKey
    vedere anche HP DriveKey
    avviabile 13 a 18
dispositivo avviabile
    creazione 12 a 18
    dischetto 12
    DiskOnKey 13 a 18
    dispositivo flash media USB 13 a 18
    HP Drive Key 13 a 18
dispositivo flash media USB, avviabile 13 a 18
Drivelock 38 a 40

E

Emergency Recovery, ProtectTools 34 a 38

F

flash ROM remoto 7
formattazione disco, informazioni importanti

H

HP Client Manager 3
HP Drive Key
    vedere anche DiskOnKey
    avviabile 13 a 18

I

immagine del software preinstallato 2
immissione
    password di accensione 25
    password di configurazione 26
impostazioni
    replica 9
indirizzi Internet, vedere siti Web
installazione remota 2
installazione remota del sistema, accesso 3

M

modifica dei sistemi operativi, informazioni importanti 19
modifica password 27

N

notifica di modifiche 5
notifica guasti 48
notifica modifica 5

O

ordinazione chiave FailSafe 44

P

partizione disco, informazioni importanti 47
password
    accensione 25
    annullamento 29
    cancellazione 28
    configurazione 26
    impostazione 24
    modifica 27
    ProtectTools 30 a 33
    sicurezza 24
password di accensione
    cancellazione 28
    immissione 25
    modifica 27
password di configurazione
    immissione 26
    ProtectTools 30
password di impostazione
    cancellazione 28
    definizione 24
    modifica 27
PCN (Proactive Change Notification) 5
personalizzazione del software 2
Preboot Execution Environment (PXE) 2
predisposizione per chiusura con cavo 47
Proactive Change Notification (PCN) 5
ProtectTools Embedded Security
    Emergency Recovery 34 a 38
    Emergency Recovery Key 31
    password
        Basic User 33
        Emergency Recovery Token 31
        Setup 30
        Take Ownership 31
protezione ROM, attenzione 6
protezione unità disco rigido 48
pulsante di accensione
    a due stati 18
    configurazione 18
pulsante di accensione a due stati 18
PXE (Preboot Execution Environment) 2

R

recupero dati crittografati 34 a 38
ripristino del sistema 8
ripristino, software 2
ROM
    flash remoto 7
    non valida 8

ROM con blocco di avvio FailSafe 8
ROM di sistema non valida 8
ROM, aggiornamento 6

S

sblocco chiusura Smart Cover 43
sensore Smart Cover 41
  impostazione 42
  livelli di protezione 41
sensore termico 49
sicurezza
  chiusura Smart Cover 42
  DriveLock 38 a 40
  funzioni, tabella 21
  impostazioni, configurazione 20
  Master Boot Record 45 a 46
  MultiBay 38 a 40
  password 24
  sensore Smart Cover 41
  Smart Cover Lock 44
sicurezza chiusura coperchio, avvertenza 42
sicurezza integrata ProtectTools 29 a 38
sicurezza Master Boot Record 45 a 46
sicurezza Multibay 38 a 40
sistemi operativi, informazioni importanti 19
Siti Web
  Altiris PC Transplant Pro 5
siti Web
  ActiveUpdate 6
  Altiris 4
  deployment PC 2
  flash ROM remoto 7
  Flash su ROM 6
  HP Client Manager 3
  HPQFlash 7
  immagini ROMPaq 6
  Proactive Change Notification 5
  replica della configurazione 12
  supporto software 19
  System Software Manager (SSM) 5
  tecnologia per l'identificazione delle impronte digitali 48
Smart Cover Lock 44
smart cover, chiusura 42
software
  aggiornamento contemporaneo di più macchine 5
  controllo risorse 20
  Drive Protection System (DPS) 48
  flash ROM remoto 7
  installazione remota del sistema 2
  integrazione 2
  notifica guasti e ripristino 48
  ripristino 2
  ROM con blocco di avvio FailSafe 8
  sicurezza Master Boot Record 45 a 46
  System Software Manager 5
  utility Computer Setup 9
spie della tastiera ROM, tabella 9
SSM (System Software Manager) 5
strumenti di clonazione, software 2
strumenti di deployment, software 2
strumento diagnostico per unità disco rigido 48
System Software Manager (SSM) 5

T

tecnologia per l'identificazione delle impronte digitali 48
temperatura interna del computer 49

U

unità disco rigido, strumento diagnostico 48
unità, protezione 48
URL (siti Web). Vedere Siti Web
utility Computer Setup 9